

# On the simple normality to base 2 of $\sqrt{s}$ , for $s$ not a perfect square

Richard Isaac  
Lehman College and Graduate Center, CUNY

## Abstract

Since E. Borel proved in 1909 that almost all real numbers with respect to Lebesgue measure are normal to all bases, an open problem has been whether simple irrational numbers like  $\sqrt{2}$  are normal to any base. This paper shows that each number of the form  $\sqrt{s}$  for  $s$  not a perfect square is simply normal to the base 2. The argument uses some elementary ideas in the calculus of finite differences.

## 1 Introduction

A number is *simply normal to base  $b$*  if its base  $b$  expansion has each digit appearing with average frequency tending to  $b^{-1}$ . It is *normal to base  $b$*  if its base  $b$  expansion has each block of  $n$  digits appearing with average frequency tending to  $b^{-n}$ . A number is called *normal* if it is normal to base  $b$  for every base. For a more detailed introductory discussion we refer to chapter 8 of [4].

The most important theorem about normal numbers is the celebrated result (1909) of E. Borel in which he proved the normality of almost all numbers with respect to Lebesgue measure. This left open the question, however, of identifying specific numbers as normal, or even exhibiting a common irrational normal number. Recently progress has been made in defining certain classes of numbers which can be proved to be normal (see [1]) but they do not include simple irrationals like  $\sqrt{2}$ , for example. The difficulty in exhibiting normality for such common irrational numbers is not

---

*AMS 2000 subject classifications.* 11K16.

*Keywords and phrases.* normal number, tail function, calculus of finite differences.

surprising since normality is a property depending on the tail of the base  $b$  expansion, that is, on all but a finite number of digits. By contrast, we mostly “know” these numbers by finite approximations, the complement of the tail.

Identification of well-known irrational numbers as normal may have interest for computer scientists. The  $b$ -adic expansion of a number normal to the base  $b$  is a sequence of digits with many of the properties of a random number table. There is thus the possibility that such numbers could be used for the generation of random numbers for the computer. This would only be possible if the digits of the normal expansion could be generated quickly enough or stored efficiently enough to make the method practical.

In this paper we exhibit a class of numbers simply normal to the base 2. More precisely, we prove

**Theorem 1** *Let  $s$  be a natural number which is not a perfect square. Then the dyadic (base 2) expansion of  $\sqrt{s}$  is simply normal.*

Consider numbers  $\omega$  in the unit interval, and represent the dyadic expansion of  $\omega$  as

$$\omega = .x_1x_2\cdots, \quad x_i = 0 \text{ or } 1. \quad (1)$$

Also of interest is the dyadic expansion of  $\nu = \omega^2$ :

$$\nu = \omega^2 = .u_1u_2\cdots, \quad u_i = 0 \text{ or } 1. \quad (2)$$

Throughout this paper it will be assumed that  $\nu$  is irrational. Then  $\omega$  is also irrational and both expansions are uniquely defined. Sometimes it will be convenient to refer to the expansion of  $\omega$  as an  $X$  sequence and the expansion of  $\nu$  as a  $U$  sequence. Define the coordinate functions  $X_n(\omega) = x_n$  and  $U_n(\omega) = u_n$  to be the  $n$ th coordinate of  $\omega$  and  $\nu$ , respectively. We sometimes denote a point of the unit interval by its coordinate representation, that is,  $\omega = (x_1, x_2, \cdots)$  or  $\nu = (u_1, u_2, \cdots)$ . Given any dyadic expansion  $.s_1s_2\cdots$  and any positive integer  $n$ , the sequence of digits  $s_n, s_{n+1}, \cdots$  is called a *tail* of the expansion. Two expansions are said to have the same tail if there exists  $n$  so large that the tails of the sequences from the  $n$ th digit are equal.

The average

$$f_n(\omega) = \frac{X_1(\omega) + X_2(\omega) + \cdots + X_n(\omega)}{n} \quad (3)$$

is the relative frequency of 1's in the first  $n$  digits of the expansion of  $\omega$ . Simple normality for  $\omega$  is the assertion that  $f_n(\omega) \rightarrow 1/2$  as  $n$  tends to

infinity. Let  $n_i$  be any fixed subsequence and define

$$f(\omega) = \limsup_{i \rightarrow \infty} f_{n_i}(\omega). \quad (4)$$

We note that the function  $f$  is a tail function with respect to the  $X$  sequence, that is,  $f(\omega)$  is determined by any tail  $x_n, x_{n+1}, \dots$  of its coordinates. In fact,  $f$  satisfies a more stringent requirement: it is an invariant function (with respect to the  $X$  sequence) in the following sense: let  $T$  be the 1-step shift transformation on  $\Omega$  to itself given by

$$T(.x_1x_2\cdots) = .x_2x_3\cdots.$$

A function  $g$  on  $\Omega$  is invariant if  $g(T\omega) = g(\omega)$  for all  $\omega$ . Any invariant function is a tail function.

The following observation will be of particular interest in the proof of Theorem 1: the average  $f_n$ , defined in terms of the  $X$  sequence, can also be expressed as a function  $h_n(\nu)$  of the  $U$  sequence because the  $X$  and  $U$  sequences uniquely determine each other. This relationship has the simple form  $f_n(\omega) = f_n(\sqrt{\nu}) = h_n(\nu)$ . A similar statement holds for any limit function  $f$  in relation 4.

**Definition:** Let  $f$  be defined as in relation 4 for any fixed subsequence  $n_i$ . We say that Condition (TU) is satisfied if  $f(\omega) = h(\nu)$  is a tail function *with respect to the  $U$  sequence* whatever the sequence  $n_i$ , that is, for any  $\omega$  and any positive integer  $n$ ,  $f(\omega)$  only depends on  $u_n, u_{n+1}, \dots$ , a tail of the expansion of  $\nu = \omega^2$ . (The notation “TU” is meant to suggest the phrase “tail with respect to the  $U$  sequence”.)

## 2 Condition (TU) implies simple normality

In this section we prove that Condition (TU) implies Theorem 1.

**Theorem 2** *If Condition (TU) is satisfied then Theorem 1 is true.*

The proof requires the following result:

**Lemma 1** *Let  $s$  be a natural number which is not a perfect square, and let  $l$  be any integer such that  $2^l > s$ . Define the points*

$$\omega_{s_1} = 1 - (\sqrt{s}/2^{2l})$$

*and*

$$\omega_{s_2} = (\sqrt{s} - 1)/2^l.$$

*Let  $f = \limsup_{i \rightarrow \infty} f_{n_i}$  where  $n_i$  is any fixed subsequence. Assume Condition (TU) is satisfied. Then  $f(\omega_{s_1}) = f(\omega_{s_2})$ .*

Proof: The numbers  $\omega_{s_i}$  are less than 1 for  $i = 1, 2$  and their squares are both irrational and are respectively given by

$$1 + s(2^{-4l}) - (2^{-2l+1}\sqrt{s}) \text{ and } (s+1)2^{-2l} - (2^{-2l+1}\sqrt{s}). \quad (5)$$

The dyadic expansions of the rational terms  $1 + s(2^{-4l})$  and  $(s+1)2^{-2l}$  in relation 5 have only a finite number of non-zero digits. Now consider the dyadic expansion of the term  $2^{-2l+1}\sqrt{s}$  (this is obtained from the expansion of  $\sqrt{s}$  by shifting the “decimal” point  $2^{2l-1}$  places to the left). To get each of the values in relation 5, this term must be subtracted from each of the larger rational terms which have terminating expansions; it is clear that the resulting numbers have expansions with the same tail, that is, the expansions of  $\omega_{s_1}^2$  and  $\omega_{s_2}^2$  have the same tail. Then Condition (TU) implies that  $f(\omega_{s_1}) = f(\omega_{s_2})$ . This finishes the proof of the Lemma.

The proof of Theorem 2 will now be completed. It is sufficient to prove simple normality for  $\lambda = \sqrt{s} - [\sqrt{s}] < 1$  where  $[t] = \text{greatest integer } \leq t$ . Define  $g_n(\omega)$  to be the average number of 0's in the first  $n$  digits of the expansion of  $\omega$ . Let  $n_i$  be any subsequence such that  $f_{n_i}(\lambda)$  converges to some value  $a$ . Now consider the point  $\lambda' = 1 - \lambda$ , and notice that for all  $j$  the  $j$ th digit of  $\lambda$  and the  $j$ th digit of  $\lambda'$  add to 1. It follows that  $g_{n_i}(\lambda')$  also converges to  $a$ . Note that the point  $\omega_{s_1}$  (as defined in Lemma 1) would have the same tail as  $\lambda'$  were we to shift a finite number of places, and therefore  $\omega_{s_1}$  and  $\lambda'$  have the same asymptotic relative frequency of 0's and 1's. The same can be asserted for  $\omega_{s_2}$  and  $\lambda$ . Thus Lemma 1 can be applied to conclude that the asymptotic averages based on  $f_{n_i}$  evaluated at the points  $\lambda$  and  $\lambda'$  are equal, that is,

$$\limsup_{i \rightarrow \infty} f_{n_i}(\lambda') = \lim_{i \rightarrow \infty} f_{n_i}(\lambda) = a.$$

But the equation  $f_n + g_n = 1$  holds for all  $n$  at all points; apply it for  $n = n_i$  at the point  $\lambda'$ , take the limit, and conclude that since  $g_{n_i}(\lambda')$  converges to  $a$ ,  $f_{n_i}(\lambda')$  converges to  $1 - a$ . The preceding relation then shows  $a = 1 - a$ , or  $a = 1/2$ . Since we have obtained convergence to  $1/2$  for  $f_{n_i}(\lambda)$  along the arbitrary convergent subsequence  $n_i$ , it follows that  $f_n(\lambda)$  itself converges to  $1/2$ . The proof of Theorem 2 is complete.

### 3 Proof that Condition (TU) is satisfied

Theorem 1 will follow from Theorem 2 if it is shown that Condition (TU) is satisfied. We do that in this section, and begin with some elementary

observations about the relationship between the digits in the expansion of  $\omega$  and those in the expansion of  $\nu = \omega^2$ .

By an *initial segment* of length  $r$  of a dyadic expansion, we refer to the string of the first  $r$  digits of the expansion. Let  $\omega_n$  be the dyadic rational formed by the initial segment of length  $n$  of  $\omega$ , that is,  $\omega_n = .x_1x_2 \cdots x_n$ .

For fixed  $r > 1$ , consider the decomposition of  $\Omega$  by the intervals

$$I_{k+1} = [k 2^{-r}, (k+1) 2^{-r}) \quad 0 \leq k \leq 2^r - 1.$$

Each of these intervals will be called an  $r$  box.

**Lemma 2** (a): If  $\omega^2 \in I_{k+1}$ , then  $.u_1u_2 \cdots u_r$ , the initial segment of length  $r$  of  $\omega^2$ , is equal to  $k 2^{-r}$ .

(b): Let  $n$  digits  $x_1, x_2, \cdots, x_n$  be specified. If

$$(.x_1x_2 \cdots x_n)^2 \text{ and } (.x_1x_2 \cdots x_n + 2^{-n})^2$$

lie in the same  $r$  box, say  $I_{k+1}$ , then, no matter how the coordinates  $x_{n+1}, x_{n+2}, \cdots$  are subsequently chosen, the point

$$\omega = .x_1x_2 \cdots x_nx_{n+1} \cdots \quad (6)$$

is such that the initial segments of length  $r$  of  $\omega^2$  and of each  $\omega_m^2$  for  $m \geq n$  are the same, with common value  $k 2^{-r}$ .

(c): Let  $\omega^2$  be irrational. Given a positive integer  $r$ , there exists a positive integer  $N_r(\omega) > 1$  such that the initial segments of length  $r$  of  $\omega^2$  and of each  $\omega_m^2$  for  $m \geq N_r$  are the same. Consequently, each of the digits  $u_1, u_2, \cdots, u_r$  is a function of the digits  $x_m, m \leq N_r$ . Moreover, the set  $\{N_r(\omega) = n\}$  is defined in terms of the coordinates  $x_1, x_2, \cdots, x_{n-1}$  of  $\omega$ .

Proof: (a): The possible values of  $.u_1u_2 \cdots u_r$  are

$$.00 \cdots 00 = 0 \cdot 2^{-r}, .00 \cdots 01 = 1 \cdot 2^{-r}, .00 \cdots 10 = 2 \cdot 2^{-r}, \cdots$$

where a digit can change only if an amount at least equal to  $2^{-r}$  is added onto the current value. Therefore each fixed value of  $.u_1u_2 \cdots u_r$  represents the left-hand endpoint of a unique  $r$  box. If  $\omega^2 \in I_{k+1}$ , then  $\omega^2$  and  $k 2^{-r}$  differ by less than  $2^{-r}$ , so the initial segment of  $\omega^2$  is still  $k 2^{-r}$ .

(b): The distance between the point

$$\omega_1 = .x_1x_2 \cdots x_n \text{ and } \omega_2 = .x_1x_2 \cdots x_n11 \cdots$$

obtained by choosing 1 for each  $x_m, m > n$  is  $2^{-n}$ . Since the point  $\omega$  of relation 6 satisfies  $\omega_1 \leq \omega \leq \omega_2$ , it follows from the assumption of part (b) that  $\omega^2$  lies in  $I_{k+1}$ . The same argument holds for  $\omega_m$  for  $m \geq n$ . The conclusion now follows from part (a).

(c): Since  $\omega^2$  is irrational,  $\omega^2$  lies in the interior of an  $r$  box. As  $m \rightarrow \infty$ ,  $\omega_m^2$  tends to  $\omega^2$  and the  $\omega_m^2$  are bounded away from the right-hand endpoint of the  $r$  box. It follows that eventually  $\omega_m^2$  and  $(\omega_m + 2^{-m})^2$  both lie in the same  $r$  box. Define  $N_r(\omega) = n$  if  $n$  is the smallest integer larger than 1 such that  $\omega_{n-1}^2$  and  $(\omega_{n-1} + 2^{-(n-1)})^2$  lie in the same  $r$  box. The assertion about initial segments follows from part (b). From the definition of  $N_r$ , the digits  $u_m, m \leq r$  are determined by giving the first  $N_r - 1$   $x$  coordinates, so the initial segment of length  $r$  of the  $u$  sequence is a function of the initial segment of length  $N_r - 1$  of the  $x$  sequence. Moreover, to determine whether a point  $\omega$  belongs to  $\{N_r(\omega) = n\}$ , one need only know the first  $n - 1$  coordinates of  $\omega$ . The last part of the assertion follows readily from part (b). This completes the proof.

The preceding result showed that an initial segment of a  $U$  sequence is determined by an initial segment of  $X$  sequences. The reverse situation is also true: an initial segment of an  $X$  sequence is determined by an initial segment of  $U$  sequences. The argument is similar to that of Lemma 2.

**Lemma 3** *Let  $\nu$  be irrational,  $\omega = \sqrt{\nu}$ , and let  $x_1, \dots, x_n$  be the first  $n$  coordinates of  $\omega$ . Then there exists an integer  $m$  depending on  $\nu$  and  $n$  such that if  $\nu' = u_1, \dots, u_m, u'_{m+1}, u'_{m+2}, \dots$  is any point whose initial  $m$  segment agrees with that of  $\nu$  but whose other coordinates may be arbitrary, then  $\omega' = \sqrt{\nu'}$  has initial segment  $x_1, \dots, x_n$ .*

Proof: The distance between  $.u_1 \dots u_j$  and  $.u_1 \dots u_j 11 \dots$  is  $2^{-j}$ . Therefore the interval with endpoints  $.u_1 \dots u_j$  and  $.u_1 \dots u_j + 2^{-j}$  contains  $\nu'$  and the endpoints converge to  $\nu$ . Decompose the unit interval into  $n$  boxes (see Lemma 2) and note that if  $\omega_1$  and  $\omega_2$  lie in the same  $n$  box, the initial segments of length  $n$  of each are the same. Since  $\omega$  is irrational, it lies in the interior of an  $n$  box. It follows that the square roots of the endpoints of the interval containing  $\nu'$  must eventually, for all sufficiently large  $j$ , be in the same  $n$  box as  $\omega$ . Thus  $\sqrt{\nu'}$  must also be in this  $n$  box. The proof is complete.

The following arguments will use some elementary ideas from the calculus of finite differences (see, e.g., [2]). We review some of the notation. Let  $v(y_1, \dots, y_l) = v(\mathbf{y})$  be a function on the  $l$ -fold product space  $S^l$  where the  $y_i \in S$ , a set of real numbers. Suppose that the variable  $y_i$  is changed by the amount  $\Delta y_i$  such that the  $l$ -tuple  $\mathbf{y}^{(1)} = (y_1, \dots, y_l)$  is taken into

$\mathbf{y}^{(2)} = (y_1 + \Delta y_1, \dots, y_l + \Delta y_l)$  in the domain of definition of  $v$ . Put  $v(\mathbf{y}^{(2)}) - v(\mathbf{y}^{(1)}) = \Delta v$ , and let

$$\begin{aligned} \Delta v_i &= v(y_1, \dots, y_{i-1}, y_i + \Delta y_i, y_{i+1} + \Delta y_{i+1}, \dots, y_l + \Delta y_l) \\ &- v(y_1, \dots, y_{i-1}, y_i, y_{i+1} + \Delta y_{i+1}, \dots, y_l + \Delta y_l). \end{aligned} \quad (7)$$

Then  $\Delta v = \sum_i \Delta v_i$  is the total change in  $v$  induced by changing all of the  $y_i$ , where this total change is written as a sum of step-by-step changes in the individual  $y_i$ . Formally, by dividing, we can write

$$\Delta v = \sum_i (\Delta v_i / \Delta y_i) \cdot \Delta y_i. \quad (8)$$

If some  $\Delta y_i = 0$ , its coefficient in relation 8 has the form  $0/0$ . Interpreting this coefficient as 0 makes the relation meaningful and true. Define the *partial difference of  $v$  with respect to  $y_i$ , evaluated at the pair  $(\mathbf{y}^{(1)}, \mathbf{y}^{(2)})$*  by

$$\frac{\Delta v}{\Delta y_i} = \Delta v_i / \Delta y_i.$$

Notice that the forward slash (/) in this relation expresses division and the horizontal slash on the left hand side is the partial difference operator. The sum of relation 8 is called the *total difference of  $v$*  evaluated at the given pair and can also be written

$$\Delta v = \sum_i \frac{\Delta v}{\Delta y_i} \cdot \Delta y_i. \quad (9)$$

The partial and total differences are the discrete analogs of the partial derivative of  $v$  with respect to  $y_i$  and the total differential, respectively, in the theory of differentiable functions of several real variables. The partial difference of  $v$  with respect to  $y_i$  at a given pair is a measure of the contribution of  $\Delta y_i$  to  $\Delta v$  when all the other  $y$  variables are held constant.

We will say that  $\omega$  and  $\nu = \omega^2$  are points that *correspond* to one another. Since corresponding points uniquely determine each other, each  $x_i$  is a function of the  $u_i$  and the average  $f_n(\omega)$  of relation 3 can be written as a function  $h_n(\nu)$  (see the Introduction). The function  $f_n$  only depends on the first  $n$  coordinates of  $\omega$ , and using a slight abuse of notation we understand by  $f_n(x_1, \dots, x_n)$  the function of  $n$  variables such that

$$f_n(x_1, \dots, x_n) = f_n(\omega) = h_n(\nu) = h_n(u_1, u_2, \dots). \quad (10)$$

Fix a point  $\omega$  and for each  $x_i$  let  $\Delta x_i$  be a given increment ( $\Delta x_i = 0, 1$ , or  $-1$ ). Let  $\omega^{(1)}$  have coordinates  $x_i + \Delta x_i$ . The changes  $\Delta x_i$  correspond

to changes  $\Delta u_i$  in the coordinates of  $\nu$ , the point corresponding to  $\omega$ , such that  $\nu$  goes into the point  $\nu^{(1)}$  with coordinates  $u_i + \Delta u_i$  corresponding to  $\omega^{(1)}$ . Assume that all  $X$  and  $U$  sequences discussed here and below represent irrational numbers. Now consider the change

$$f_n(\omega^{(1)}) - f_n(\omega) = \Delta f_n = \Delta h_n = h_n(\nu^{(1)}) - h_n(\nu),$$

where the right hand side can be written

$$\Delta h_n = h_n(u_1 + \Delta u_1, u_2 + \Delta u_2, \dots) - h_n(u_1, u_2, \dots). \quad (11)$$

Recall that the capital letter notation  $X_i$  and  $U_i$  denotes the  $i$ th coordinate variable of  $\omega$  and  $\nu$ , respectively. This notation will be convenient when small letters may be reserved to denote particular values.

**Lemma 4** *At the pair  $(\nu, \nu^{(1)})$ ,  $\Delta h_n$  can be represented as a total difference*

$$\begin{aligned} \Delta h_n &= h_n(u_1 + \Delta u_1, u_2 + \Delta u_2, \dots) - h_n(u_1, u_2, \dots) \\ &= \sum_{i \geq 1} \frac{\Delta h_n}{\Delta U_i} \Delta U_i = \sum_{i \geq 1} (\Delta h_{n,i} / \Delta U_i) \Delta U_i, \end{aligned} \quad (12)$$

where  $\Delta U_i = \Delta u_i$  and

$$\begin{aligned} \Delta h_{n,i} &= \Delta h_{n,i}(\nu, \nu^{(1)}) = \\ &= h_n(u_1, \dots, u_{i-1}, u_i + \Delta u_i, u_{i+1} + \Delta u_{i+1}, \dots) - \\ &= h_n(u_1, \dots, u_{i-1}, u_i, u_{i+1} + \Delta u_{i+1}, \dots). \end{aligned} \quad (13)$$

*The formally infinite sum of relation 12 reduces to a finite sum when evaluated at the pair  $(\nu, \nu^{(1)})$ , that is, given the pair, there exists an integer  $m$  such that the partial differences  $\Delta h_{n,i} / \Delta U_i = 0$  for all  $i > m$ . The number of non-vanishing terms in the sum depends on the pair chosen and on  $n$ .*

Proof: The function  $h_n = f_n$  only depends on the initial segment of length  $n$  of  $\omega$ . Given  $\nu$ , Lemma 3 proves the existence of an integer  $m$  such that for all  $i > m$ , the points with coordinates

$$\begin{aligned} u_1, \dots, u_{i-1}, u_i + \Delta u_i, u_{i+1} + \Delta u_{i+1}, \dots \quad \text{and} \\ u_1, \dots, u_{i-1}, u_i, u_{i+1} + \Delta u_{i+1}, \dots \end{aligned} \quad (14)$$

correspond to  $X$  sequences having the same initial segment of length  $n$  as  $\omega$ . Consequently, for  $i > m$  the difference terms in relation 13 are equal and the partial differences evaluated at the given pair vanish. The argument is



thus reduced to the observations leading to relations 7 and 8, and the proof is finished.

Since  $X_j$  is a function of the  $U$  variables for all  $j$ , an argument similar to the above shows that there is a representation analogous to relation 12 of the form

$$\Delta X_j = \sum_{i \geq 1} \frac{\Delta X_j}{\Delta U_i} \Delta U_i = \sum_{i \geq 1} (\Delta X_{j,i} / \Delta U_i) \Delta U_i, \quad (15)$$

where  $\Delta X_{j,i}$  is derived from  $\Delta X_j$  in the same way as  $\Delta h_{n,i}$  is derived from  $\Delta h_n$  (see relation 13). At a given pair this representation also reduces to a finite sum by Lemma 3.

In similar fashion, representations in terms of the  $X$  variables may be written. At the pair  $(\omega, \omega^{(1)})$  we obtain the following relations analogous to relations 12 and 15:

$$\Delta h_n = \Delta f_n = \sum_{j \geq 1} \frac{\Delta f_n}{\Delta X_j} \Delta X_j = \sum_{j \leq n} \frac{1}{n} \Delta X_j, \quad (16)$$

and

$$\Delta U_i = \sum_{j \geq 1} \frac{\Delta U_i}{\Delta X_j} \Delta X_j = \sum_{j \geq 1} (\Delta U_{i,j} / \Delta X_j) \Delta X_j, \quad (17)$$

where  $\Delta U_{i,j}$  is defined similarly to  $\Delta h_{n,i}$  and  $\Delta X_{j,i}$ .

Now fix the positive integer  $k$  and refer to relation 12. It will be seen that at the pair  $(\nu, \nu^{(1)})$  and for any subsequence  $n_l$ ,  $\limsup_l \Delta h_{n_l}$  does not depend on the values of  $\Delta U_i$ ,  $i \leq k$ . This is what must be shown to prove the validity of Condition (TU), that is, that the influence of any initial segment of the  $U$  variables on  $h_n$  dies out in the limit. To this end we first observe that either the  $X$  or the  $U$  variables may be taken as independent variables, with the other set dependent on them. We take the  $X$  variables as independent. We now rewrite relation 12 in terms of the  $X$  variables, using the dependence relation of  $U$  on  $X$ . The following result is an analog of the chain rule for differentiable functions of several real variables.

**Lemma 5** *Let the  $U$  variables be functions of the independent  $X$  variables. Then for each  $j$  the following relations are valid evaluated at any pair:*

$$\Delta h_n = \sum_j \left( \sum_i \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} \right) \Delta X_j, \quad (18)$$

and

$$\sum_i \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} = \frac{\Delta h_n}{\Delta X_j} = \frac{1}{n} \text{ for } j \leq n \text{ and } = 0 \text{ for } j > n. \quad (19)$$

Proof: Start with relation 12, substitute relation 17 and interchange the order of addition (possible because of the finiteness of the sums) to get:

$$\begin{aligned}\Delta h_n = \sum_i \frac{\Delta h_n}{\Delta U_i} \Delta U_i &= \sum_i \frac{\Delta h_n}{\Delta U_i} \left( \sum_j \frac{\Delta U_i}{\Delta X_j} \Delta X_j \right) \\ &= \sum_j \left( \sum_i \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} \right) \Delta X_j,\end{aligned}\quad (20)$$

and this is relation 18. To prove relation 19, take the partial difference on both sides of relation 18 with respect to  $X_{j_0}$  for a fixed index  $j_0$ . Note that the partial difference of a sum evaluated at a given pair is additive, so that

$$\frac{\Delta h_n}{\Delta X_{j_0}} = \sum_j \left( \sum_i \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} \right) \frac{\Delta X_j}{\Delta X_{j_0}}, \quad (21)$$

where the left hand side of relation 21 is equal to  $1/n$  or 0 depending on whether  $j_0 \leq n$  or  $> n$ . The variables  $X_j$  are independent. This means that a change in  $X_{j_0}$  does not cause a change in  $X_j, j \neq j_0$ , that is

$$\frac{\Delta X_j}{\Delta X_{j_0}} = 0, j \neq j_0 \text{ and } = 1 \text{ if } j = j_0.$$

Relation 21 thus reduces to relation 19.

**Lemma 6** *Let  $k$  be a fixed index and let the pair  $(\nu, \nu^{(1)})$  be given as in Lemma 4. Then at any pair  $(\nu, \nu^{(*)})$  for which  $\nu^{(*)}$  has the same tail as  $\nu^{(1)}$  starting from index  $(k+1)$ , we have*

$$\limsup_n \Delta h_n = \limsup_n \sum_{i>k} \frac{\Delta h_n}{\Delta U_i} \Delta U_i. \quad (22)$$

*The right hand side of relation 22 is the same, term by term, as the right hand side of relation 12 if  $\Delta U_i, i \leq k$  are set equal to 0 there. Thus  $\limsup_n \Delta h_n$  is constant over all such pairs  $(\nu, \nu^{(*)})$  and does not depend on the values of  $\Delta U_i, i \leq k$ . Relation 22 remains true if the limit superior is taken over any subsequence  $n_l$  rather than the entire sequence. In addition, in relation 12 we have*

$$\lim_n \Delta h_{n,k} = \lim_n \frac{\Delta h_n}{\Delta U_k} = 0.$$

Proof: Let  $k$  be given, and consider the set  $S_1$  of the  $2^k$  points in  $U$  space for which the tail starting from the coordinate  $(k+1)$  is the same as that of  $\nu^{(1)}$  but the initial segment of length  $k$  runs through all possible values. Let  $S$  be the set of the  $2^k$  pairs  $(\nu, \nu^{(*)})$  where  $\nu^{(*)} \in S_1$ . According to Lemma 2 there exists  $N$  such that  $U_i, i \leq k$  is a function of the corresponding  $X_j, j \leq N$  for all points in  $S_1$ . Relation 19 implies that at any pair whatsoever

$$\lim_n \sum_{j \leq N} \left( \sum_i \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} \right) \Delta X_j = 0. \quad (23)$$

Relation 18 then gives

$$\begin{aligned} \limsup_n \Delta h_n &= \limsup_n \Delta f_n = \limsup_n \sum_{j > N} \left( \sum_i \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} \right) \Delta X_j = \\ \limsup_n \left[ \sum_{j > N} \left( \sum_{i \leq k} \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} \right) \Delta X_j + \sum_{j > N} \left( \sum_{i > k} \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} \right) \Delta X_j \right]. \end{aligned} \quad (24)$$

We claim that at pairs of  $S$  the first of the two double sums within the bracket on the right hand side of relation 24 vanishes. The reason is that  $U_i, i \leq k$  only depend on  $X_j, j \leq N$  so that

$$\frac{\Delta U_i}{\Delta X_j} = 0 \text{ for } i \leq k \text{ and } j > N.$$

It follows that we have

$$\limsup_n \Delta f_n = \limsup_n \sum_{j > N} \left( \sum_{i > k} \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} \right) \Delta X_j. \quad (25)$$

It should be noted that the partial differences of  $h_n$  with respect to  $U_i$  for  $i > k$  in relation 25 at a pair of  $S$  are the same as the corresponding terms in relation 12 at the pair  $(\nu, \nu^{(1)})$ ; this is immediate by comparison using relation 13. Also observe that relations 24 and 25 also hold if the limit superior had been taken over any subsequence  $n_l$  instead of over the entire sequence.

Let us define

$$h_n^{(k)}(U_{k+1}, U_{k+2}, \dots) = h_n(u_1, \dots, u_k, U_{k+1}, U_{k+2}, \dots)$$

where we recall that  $u_1, \dots, u_k$  is the initial segment of length  $k$  of  $\nu$  and  $U_{k+1}, U_{k+2}, \dots$  are variables. Then at any pair in  $S$  the value of  $\Delta h_n^{(k)}$  is

constant, namely

$$\Delta h_n^{(k)} = \sum_{i>k} \frac{\Delta h_n}{\Delta U_i} \Delta U_i, \quad (26)$$

where again we observe that the terms are the same as the corresponding terms in relation 12. Now for any pair in  $S$  we may also write a representation of  $\Delta h_n^{(k)}$  in terms of the  $X$  variables:

$$\Delta h_n^{(k)} = \sum_{j \geq 1} \frac{\Delta h_n^{(k)}}{\Delta X_j} \Delta X_j. \quad (27)$$

For  $i \leq k$ , the partial difference of  $\Delta h_n^{(k)}$  with respect to  $\Delta U_i$  is equal to 0, and so for any  $j$

$$\frac{\Delta h_n^{(k)}}{\Delta X_j} = \sum_{i \geq 1} \frac{\Delta h_n^{(k)}}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} = \sum_{i>k} \frac{\Delta h_n^{(k)}}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} = \sum_{i>k} \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j}. \quad (28)$$

Put relation 28 into relation 27 to get

$$\limsup_n \Delta h_n^{(k)} = \limsup_n \sum_{j \geq 1} \left( \sum_{i>k} \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} \right) \Delta X_j. \quad (29)$$

The argument leading to relation 29 goes through without change for any subsequence  $n_l$  used instead of the entire sequence. The left hand side of relation 29 does not depend on any fixed coordinate  $X_{j_0}$ , even if the limsup is taken over any subsequence. If the coefficients of  $\Delta X_{j_0}$  in relation 29

$$\sum_{i>k} \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_{j_0}} \quad (30)$$

do not converge to 0, then there is a subsequence converging to a non-zero value. This would mean that the limsup of the right hand side of relation 29 along this subsequence would depend on the value of  $\Delta X_{j_0}$ . But this contradicts what is known for the left hand side of this relation. So the terms in relation 30 converge to 0 and this holds for arbitrary indices  $j_0$ , permitting us to rewrite relation 29 as

$$\limsup_n \Delta h_n^{(k)} = \limsup_n \sum_{j>N} \left( \sum_{i>k} \frac{\Delta h_n}{\Delta U_i} \frac{\Delta U_i}{\Delta X_j} \right) \Delta X_j. \quad (31)$$

The right hand sides of relations 31 and 25 are the same. These relations together with relation 26 prove that at any pair of  $S$

$$\limsup_n \Delta f_n = \limsup_n \Delta h_n = \limsup_n \Delta h_n^{(k)} = \limsup_n \sum_{i>k} \frac{\Delta h_n}{\Delta U_i} \Delta U_i. \quad (32)$$

The argument leading to relation 32 goes through without change for any subsequence  $n_l$  used instead of the entire sequence. This relation thus expresses  $\limsup_l \Delta h_{n_l}$  for an arbitrary subsequence at any pair of  $S$  in terms of a function of the  $U_i$  variables for  $i > k$  which is constant at pairs in  $S$ . This function is the same as that in relation 12 if  $\Delta U_i = 0$ ,  $i \leq k$ . It will follow that  $\lim_n \Delta h_{n,k} = 0$  in relation 12; the argument is similar to one given above. Without loss of generality take  $k = 1$  and consider the representation of  $\Delta h_n$  at  $(\nu, \nu^{(1)})$  given by relation 12. If there is a subsequence  $\Delta h_{n_l,1}$ , say, converging, if possible, to a non-zero value, then relation 12 proves  $\limsup_l \Delta h_{n_l}$  dependent on  $\Delta U_1$ , but this contradicts relation 32 for subsequences. Therefore  $\Delta h_{n,1}$  converges to 0, and the proof of the lemma is complete.

We are ready to summarize the foregoing results into a formal statement that Condition (TU) is satisfied.

**Lemma 7** *(Condition (TU) is satisfied) Let  $f_n(\omega)$  be the average of relation 3. Let  $n_i$  be any fixed subsequence. Then the function  $f = \limsup_{i \rightarrow \infty} f_{n_i}$  is a tail function with respect to the variables  $U_1, U_2, \dots$ , that is, for any given positive integer  $k$ , the function  $f$  can be written as a function of  $U_{k+1}, U_{k+2}, \dots$ . Consequently, if  $\omega$  and  $\omega^{(1)}$  have corresponding points  $\nu$  and  $\nu^{(1)}$  with the same tail, then  $f(\omega) = f(\omega^{(1)})$ .*

Proof: Suppose that  $\nu$  and  $\nu^{(1)}$  have the same tail starting from index  $k + 1$ . Apply Lemma 6 to conclude that  $\limsup_n \Delta h_n = \limsup_n \Delta f_n$  only depends on the values of  $\Delta U_i$  for  $i > k$  and has the representation given by relation 22. This proves the assertion and concludes the proof of Theorem 1.

We end our discussion by mentioning the problem of extending Theorem 1 from simple normality to normality. It appears that an approach similar to the one given here will work. We hope to have completed results soon.

## References

- [1] David H. Bailey and Richard E. Crandall, *Random Generators and Normal Numbers*, to appear in *Experimental Mathematics* (also see first author's web site).
- [2] Samuel Goldberg, *Introduction to Difference Equations*, John Wiley, 1958.
- [3] G. H. Hardy, *A Course of Pure Mathematics*, Cambridge University Press, 1952.
- [4] Ivan Niven, *Irrational Numbers*, Mathematical Association of America (Carus Mathematical Monograph), distributed by John Wiley, 1956.